Department of Homeland Security
Information Analysis and Infrastructure Protection
Daily Open Source Infrastructure Report for 02 September 2003

Current Nationwide Threat Level is
ELEVATED
Significant Risk of Terrorist Attacks
For info click here
www.whitehouse.gov/homeland

Daily Overview

- The Associated Press reports federal prosecutors said last Friday, that U.S. officials have broken up a money laundering ring in Florida that processed at least $30 million for drug traffickers over the past four years. (See item 10)
- The Associated Press reports the Port of Miami, one of the busiest cruise ship hubs in the world, was shut down for about two hours Friday, August 29, after ammonia leaked from a refrigerated shipping container in a storage area. (See item 12)
- The Denver Post reports Colorado's largest blood bank voluntarily recalled more than 1,700 units of blood, fearful that West Nile virus had seeped into its supply in the days before screening tests began on July 1. (See item 20)

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: Elevated, Cyber: Elevated
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://esisac.com]

1. *August 29, Reuters* — **Duke Catawba 1 nuke to stay off line for days. Duke Energy Co. said on Friday, August 29, that its 1,129 megawatt Catawba 1 nuclear unit will remain shut for days during repairs after it automatically tripped off line earlier that day.** Catawba 1, about six miles northwest of Rock Hill, SC, tripped off line following a problem with a temperature protection system. Meanwhile, the adjacent 1,129 MW Unit 2 nuclear continued to

operate at full power.
Source: http://biz.yahoo.com/rm/030829/utilities_duke_catawba_2.html

2. *August 29, Associated Press* — **Energy panel recommends power grid fixes.** An influential energy panel has called for new investment incentives and a bigger role for federal regulators to make the nation's "seriously overloaded" power system more reliable. The recommendations from the National Commission on Energy Policy, issued on Thursday, August 29, were issued days ahead of congressional hearings on the nation's worst blackout two weeks ago. **They include empowering the Federal Energy Regulatory Commission to mandate grid reliability standards and impose higher, uniform charges to pay for investments in transmission lines. To limit grid vulnerability to a terrorist attack, the panel said the industry should maintain "stockpiles of critical equipment."** Originally built to handle the flow of electricity from monopolistic utilities serving a local customer base, the grid has been expanded over the decades to handle power transactions that crisscross the continent, giving generators the opportunity to sell their juice for the highest possible price.
Source: http://www.nytimes.com/aponline/national/AP−Blackout−Fixing− the−Grid.html

3. *August 29, Associated Press* — **TVA issues alert after problem with nuclear reactor. During a test on Thursday, August 28, a reactor at the Sequoyah Nuclear Plant was shut down, but because it did shut down as designed, the Tennessee Valley Authority issued an alert that same day.** The alert was canceled after being in effect for about four hours. Operators said plant systems are responding as expected for a unit in shutdown mode. Plant staff are continuing to review the cause of the shutdown. No injuries were reported, and radioactive releases were not above normal. An alert is the second level of nuclear emergency classifications and is issued when an incident could reduce the plant's safety. The nuclear plant, which has two reactors, is on the Tennessee River about 18 miles northeast of Chattanooga, TN.
Source: http://www.tennessean.com/local/archives/03/08/38437386.shtml?Element_ID=38437386

4. *August 29, Reuters* — **UK National Grid says double power fault was unusual. The power system failure that plunged London into chaos on Thursday, August 28, was an unusual occurrence that is unlikely to happen again, Britain's bulk electricity carrier National Grid Transco said on Friday, August 29.** "Localized protection equipment worked and isolated the faults," the spokesperson said. "Under normal circumstances you can re−route the power when a fault like this occurs, but because two happened in quick succession, our ability to do that was restricted. It's very unusual to get two faults together." Two system faults showed up in National Grid's control rooms at around 5:20 GMT on Thursday, and occurred on a 275 kilovolt network. The grid took action to shut down power to the affected areas in a move that cut off three key substations. These substations reduced the voltage again from the transitional 275 kilovolt network to lower levels for delivery to the local distribution networks that work independently of National Grid. Engineers were successful in re−routing power about 32 minutes later, but it was almost an hour before the main local power provider affected, EDF Energy, was able to bring all its customers back on line.
Source: http://hsweb01.screamingmedia.com/PMA/pma_newsarticle1_reuters.htm?SMDOCID=reuters_pma_2003_08_29_eng−reuters_pma_UK−NATL−GRID−SAYS−DOUBLE−POWER−FAULT−WAS−A−FREAK&SMContentSet=0

5. *August 28, The Record (NJ)* — **Probe of blackout could take many weeks, Energy Secretary declares.** At a news briefing on Wednesday, August 27, U.S. Secretary of Energy Spencer Abraham expressed confidence that investigators would pinpoint the cause of the August 14 blackout, but said the process could take many weeks. **Investigators are going through a "staggering amount of data" looking for answers to three questions, Abraham said: What triggered the blackout, why did it spread so rapidly, and what can be done to prevent a recurrence?** The meeting concentrated on establishing lines of communication and the process for an investigation that will take weeks, "hopefully not months," the secretary said. "The facts will drive any recommendations we make, so I will not prejudge what they may be," Abraham said. "Any recommendation which our joint U.S.−Canada task force makes will likely focus on technical standards for operation and maintenance of the grid and for management and performance in order to quickly correct the problems we identify." The task force will issue "regular reports," but not until it is comfortable with the accuracy of its findings, Abraham said.
Source: http://hsweb01.screamingmedia.com/PMA/pma_newsarticle1_krt.htm?SMDOCID=knightridder_2003_08_28_krtbn_0000−0547−HK−BLACKOUT&SMContentSet=0

6. *August 28, Reuters* — **NRC inspects FirstEnergy Ohio nuke after blackout. The Nuclear Regulatory Commission (NRC) said on Thursday, August 28, it has launched a "special inspection" of FirstEnergy Corp.'s Perry nuclear power plant in Ohio following problems restarting it after the August 14−15 blackout.** The 1,320 megawatt plant, one of nine reactors in the U.S. Midwest and Northeast knocked offline by the blackout, resumed operation Wednesday, August 20, and was back at full power by Monday, August 25. But the NRC said the unit experienced two equipment problems during restart, prompting the extra inspections. The commission said in a statement a small support system pump had failed to operate properly during restart and that one of the plant's emergency generators did not provide correct voltage during a routine test on August 21. Neither problem posed a public health risk, the company said.
Source: http://reuters.com/financeNewsArticle.jhtml?type=governmentFilingsNews&storyID=3353994

[Return to top]

Chemical Sector

7. *August 29, United States Chemical Safety and Hazard Investigation Board* — **Acid spill at Honeywell plant hurts two workers. Two Honeywell employees were hospitalized Wednesday after they were exposed to hydrofluoric acid while cleaning equipment at the Lupine Street facility in Baton Rouge, LA, a company spokesman confirmed.** Three pounds of hydrofluoric solution spilled in the accident, said Jeffrey Meyers, emergency response manager with the Department of Environmental Quality. The acid caused a 6−inch burn on the forearm of one employee and caused inhalation problems to another standing nearby. **"They were breaking down or doing repair work on a hydrofluoric line and the product that was left in the line sprayed," Fire Department spokesman Howard Ward said. This is the third accident at the chemical plant in just more than three weeks.** Honeywell will be cited with a civil violation by State Police for failure to report Wednesday's

accident in a timely manner, Trooper Johnnie Brown confirmed. EMS was called about 11:15 a.m., an EMS spokesman said. After the spill July 29, a Honeywell worker died the next day. Eight people suffered injuries in the July 20 spill.
Source: http://www.chemsafety.gov/circ/post.cfm?incident_id=6705

8. *August 26, United States Chemical Safety and Hazard Investigation Board* — **Ammonia leak causes evacuation. It was a scare for several Valley families, in the town of Sanger, CA, Tuesday evening, who were evacuated from their homes after a toxic spill. Fire officials say an ammonia pump malfunctioned at the Cal−Fresh plant, sending anhydrous ammonia gas into the air.** Workers told neighbors to evacuate and called for help. Fire crews shut off the leak and people were allowed back in their homes, but not before some were affected by the fumes. **People could smell the ammonia several blocks away, but the fire chief says the accident could've been much worse. Anhydrous ammonia can be extremely dangerous if too much of it is inhaled.**
Source: http://www.chemsafety.gov/circ/post.cfm?incident_id=6702

[Return to top]

Defense Industrial Base Sector

9. *August 29, Associated Press* — **Report says Air Force computers failed to flag unauthorized sales. In a report by the Government Accounting Office (GAO) released on Thursday, August 28, computer glitches by the Air Force allowed some foreign countries to receive classified or sensitive parts they weren't supposed to have, and the Air Force didn't have any procedures for trying to recover the parts.** The Pentagon doesn't allow some parts to be sold to other countries to keep them from falling into the hands of enemies or terrorists and to protect American advantages in technology. **But an Air Force computer system used for processing foreign orders for spare parts didn't always prevent banned parts from being shipped, the GAO study found. The computer system incorrectly approved 35 of 123 requests for restricted parts, including target−detecting devices and restricted communications security parts, the report said.** Air Force officials responding to the report said most of the problems had been fixed or were being corrected.
Source: http://www.ajc.com/news/content/news/0803/29glitch.html

[Return to top]

Banking and Finance Sector

10. *August 29, Associated Press* — **U.S. breaks alleged money laundering ring in Miami. U.S. officials have broken up a money laundering ring in Florida that processed at least $30 million for drug traffickers over the past four years, federal prosecutors said Friday, August 29.** Attorney General John Ashcroft has said the ring was one of the world's most wanted drug and money laundering organizations. The Drug Enforcement Administration said the arrests represent a "re−energized effort" to attack the financial underpinnings of drug cartels.
Source: http://abcnews.go.com/wire/US/ap20030829_957.html

11. *August 28, ZDNet* — **Latest e−mail scam targets National Australia Bank.** In what has become a weekly event, Australian consumers have been targeted by another e−mail scam −− the latest targets National Australia Bank (NAB) customers. The scam uses the same, grammatically incorrect message as previous scams that have targeted St. George and Westpac banking customers. "Dear valued customer," it reads, "our new security system will help you to avoid frequently fraud transactions and to keep your investments in safety." **The e−mail encourages recipients to click a link in the body of the message which takes them to a site that mimics the NAB website. Unbeknownst to the user, the site they are logging in to is not an official bank website, but a "ghost" site set up to capture users login and password details. A campaign has been launched to educate customers about such scams, especially warning them to never give out personal information and passwords.**
Source: http://www.zdnet.com.au/newstech/security/story/0,2000048600 ,20277852,00.htm

[Return to top]

Transportation Sector

12. *August 29, Associated Press* — **Ammonia leak briefly shuts Port of Miami. The Port of Miami, one of the busiest cruise ship hubs in the world, was shut down for about two hours Friday after ammonia leaked from a refrigerated shipping container in a storage area, fire officials said. One worker was injured.** The ammonia escaped when a valve on the container malfunctioned at about 8 a.m., said Lt. Eugene Germain Jr., a Miami−Dade Fire Rescue spokesman. **The port reopened after the leak was stopped and a vapor cloud that had formed over the area dissipated.** Ammonia−−used as a cleaner and in fertilizers and manufacturing, as well as refrigeration−−is corrosive and can cause burns when touched or when vapors are inhaled. It is generally not considered to be a danger to explode or ignite unless the gas is highly concentrated. Tim Gallagher, a spokesman for Carnival Cruise Lines, said that about 2,000 passengers aboard one returning ship were kept on board because of the leak but that it posed no danger to them. **The Port of Miami, in addition to being a stopping point for more than 3 million cruise ship passengers annually, is a major cargo port, with more than 8 million tons passing through each year.**
Source: http://www.ajc.com/news/content/news/ap/ap_story.html/National/AP.V4267.AP−Port−Ammonia−Le.html

13. *August 29, San Francis Chronicle* — **Israel has anti−missile plan for jets. Prime Minister Ariel Sharon has ordered the installation of anti−missile systems on Israel's El Al and Arkia airliners,** according to Israeli government officials and defense contractors with knowledge of the decision. Capt. James Shilling, a pilot and spokesman on legislative and security issues for the Coalition of Airline Pilots Associations, based in Washington, welcomed Israel's decision. **An alternative to the system being deployed by the Israelis, according to experts inside the Department of Defense and the Department of Homeland Security, is an anti−missile system called "directed infrared countermeasures."** It detects a missile launch by identifying ultraviolet radiation in the missile plume and then firing pulses of light onto the missile's homing device. The pulses "confuse" the rocket's guidance system, making it veer away from its intended victim. The most effective of these systems uses lasers to generate the light pulses.

Source: http://www.sfgate.com/cgi−bin/article.cgi?file=/c/a/2003/08/ 29/MN296631.DTL

14. *August 29, Associated Press* — **Federal investigators looking at similarities between plane crashes. A spokesman for the National Transportation Safety Board says that a North Carolina plane crash that claimed 21 lives earlier this year and a fatal plane crash off Cape Cod this week that killed two pilots had a number of commonalities.** Both planes were the same type of Beechcraft, and both had undergone recent maintenance on similar pieces of equipment. The spokesman also says control problems were evident just after take−off. But he says there is nothing to suggest a fleet−wide problem. In this week's crash, the plane was headed to Albany, New York from the Hyannis airport when it crashed into the water. In the North Carolina incident, the plane crashed into a hangar shortly after taking off from Charlotte−Douglas International Airport.
Source: http://www.wkyt.com/Global/story.asp?S=1422819

[Return to top]

Postal and Shipping Sector

Nothing to report.
[Return to top]

Agriculture Sector

15. *August 29, Iowa Ag Connection* — **New course studies crop bioterrorism. A new graduate course this fall semester at the Iowa State College of Agriculture will assess the threat of crop bioterrorism in Iowa. It is the first graduate course taught in the U.S. to address crop bioterrorism, said Forrest Nutter, plant pathology professor and member of the bioterrorism committee of the American Phytopathological Society.** The course includes the study of microorganisms and insect pests that can directly affect the health and productivity of crops. Students also will develop a list of criteria to rank the importance of biotic pathogens and insect pests that could threaten Iowa agriculture and prepare a prioritized list of pathogens and pests that most threaten the food security and economic stability of Iowa agriculture. Although it is a graduate course, Nutter said undergraduate students are welcome to participate in the seminars. Eventually, he said he may develop the course into an undergraduate offering.
Source: http://www.iowaagconnection.com/story−state.cfm?Id=679&yr=20 03

16. *August 29, Agriculture.com* — **Soybean cyst nematode spreads to North Dakota. The first verified cases of soybean cyst nematode (SCN) in North Dakota have been found in several fields in Richland County, according to Carl Bradley, North Dakota State University (NDSU) plant pathologist.** Richland is in the southeast corner of the state. Because SCN is sometimes difficult to detect, they don't know just how extensive an area of the state is infested. "We think it could have been in the infected fields for five to seven years before we detected it because it takes awhile to build up," says Berlin Nelson, NDSU plant pathologist. "The disease was reported in Minnesota in 1978 and in South Dakota in 1995," Bradley says. "Given that the disease was so close, we knew it was only a matter of time before it would hit North Dakota." Soybean cyst nematode is the most important soybean disease in the country,

NDSU says. **In 2002, estimated losses from SCN in the U.S. totaled 133 million bushels. "Losses of 15 to 30 percent have been reported even when there are no obvious above−ground symptoms," Bradley says. "When the nematode is abundant, losses can exceed 20 bushels per acre. In extreme cases, almost no crop will be produced."**
Source: http://www.agriculture.com/default.sph/AgNews.class?FNC=goDetail__ANewsindex_html___50516___1

17. *August 28, Crop Decisions* — **USDA to begin issuing permits for Canadian beef imports. The U.S. Department of Agriculture (USDA) on Thursday will begin issuing the first permits for imports of Canadian beef since trade was suspended in May because of one confirmed case of mad cow disease in Alberta, according to a USDA official.** "We are going to start issuing permits today," said David Hegwood, special trade adviser at USDA. Hegwood added it could take a few days before trucks carrying beef from Canada will cross the border into the United States. "It depends in part on getting the inspections done on the Canadian side and whatever time it takes with commercial process work," Hegwood said. **Hegwood said USDA was not anticipating a "tremendous surge" in shipments, which include boneless beef from cows under 30 months old.** He said he had no details on how much beef initially would be imported. The USDA announced on August 8 it would begin easing a three month trade ban on Canadian beef and cattle, starting with what it considers "low−risk" beef. The department is looking at the possibility of allowing some live cattle into the U.S., but it could be several months before that trade resumes.
Source: http://www.cropdecisions.com/show_story.php?id=21036

[Return to top]

Food Sector

18. *August 29, Engineer* — **Bacterial analysis with beads. The engineers behind a tiny testing system that uses magnetic bead technology to isolate and identify harmful food−borne bacteria hope to begin full−scale production soon. The system, being tested in hospitals in Cardiff and Liverpool, England, aims to speed up the bacterial analysis process, an important factor in halting outbreaks of food poisoning before they get out of hand.** The small disposable cartridge binds bacteria from contaminated samples to magnetic beads, which are themselves captured by small magnets built into the system. Chemical reagents are then automatically applied, creating a luminescence that can be detected via optical electronic analysis to check for pathogens such as campylobacter, listeria, salmonella, and clostridium. The system is controlled and monitored via a standard PC equipped with custom−developed software, meaning analysis can be carried out on−site at the point of contamination. This reduces analysis to within a working day, allowing treatment and appropriate anti−contamination measures to start immediately. The minimal manual intervention needed to operate the system also reduces the risk of infection to those carrying out the analysis, they say.
Source: http://www.e4engineering.com/item.asp?id=49710&type=news

[Return to top]

Water Sector

19. *August 29, Water Tech Online* — **Water counter−terrorism funds allocated by EPA. The Environmental Protection Agency (EPA) has allocated nearly $5 million in state and tribal assistance grants to assist drinking water systems across the nation bolster their defenses against possible terrorism.** The grants are in continued support of counter−terrorism coordination with state, local, and federal governments, which began under a 2002 program This coordination is to ensure drinking water utilities receive technical assistance and training on homeland security issues, including vulnerability assessments and emergency response plans. **Along with the grant allocation, the EPA is also funding a $2 million program in conjunction with the Office of Water. The Environmental Technology Verification (ETV) program is developing innovative protocols and testing technologies to monitor the safety and security of the nation's drinking water systems and supplies.** The first round of verification testing will commence soon on one point−of−use (POU) reverse osmosis combination unit. Two other vendors' products are planned for testing later in the fall. These devices should provide dual benefits to homeland security by offering an additional level of protection from potential biological and chemical contamination of drinking water supplies. Source: http://www.watertechonline.com/news.asp?mode=4&N_ID=42622

[Return to top]

Public Health Sector

20. *August 29, Denver Post* — **Virus prompted blood recall. Colorado's largest blood bank voluntarily recalled more than 1,700 units of blood, fearful that West Nile virus had seeped into its supply in the days before screening tests began on July 1.** Bonfils Blood Center decided on July 17 to recall 1,794 blood products. Despite the pre−emptive action, Dr. William Dickey, Bonfils president, said the risk that the blood carried West Nile was "infinitesimally small," since few infections had been reported then. **Meanwhile, the Nebraska health department is investigating its first suspected case of West Nile virus transmitted by tainted blood transfusions.** And Colorado this week learned that one of its more than 800 West Nile victims gave blood shortly before experiencing symptoms of the infectious disease. Colorado state epidemiologist John Pape said the state is tracking down when and where the person donated blood and will alert the appropriate blood center. **Last year, 23 people nationwide got West Nile from tainted transfusions. To reduce the chances of that happening again this year, the Food and Drug Administration put a new blood test on the fast track so it could be used before West Nile season began anew.**
Source: http://www.denverpost.com/Stories/0,1413,36~53~1598328,00.ht ml

[Return to top]

Government Sector

21. *August 29, Tucson Citizen* — **GAO reports: checking of border crossers inconsistent at ports of entry. Vulnerabilities at ports of entry around the country increase the risk of illegal entry and more resources are needed along ports of entry (POE) at our borders due to the threat of terrorism, according to a letter issued by the General Accounting Office**

(GAO), the investigative arm of congress. The letter was written to Robert Bonner, commissioner of the Bureau of Customs and Border Protection. GAO's Assistant Director Michael Dino said the material was deemed sensitive but confirmed that one of the six ports of entry inspected along the southern border for the report was in Nogales, Ariz. Immigration and Customs Enforcement Spokesman Roger Maier said many of the "separate agency" structures prior to the merging of several immigration and customs agencies March 1 is what caused the consistency and uniformity problems, which he's confident are behind the new agency, a "unified border security organization." **The letter states the collection, analysis and use of intelligence information is impeded by a lack of time and training for agents at ports. "Given the threat of terrorism confronting the country, having and using intelligence information effectively at land border POEs has never been more important," the letter stated.** GAO letter: http://www.gao.gov/new.items/d031084r.pdf
Source: http://www.tucsoncitizen.com/breaking/8_29_03gaoreport.html

[Return to top]

Emergency Services Sector

22. *September 01, WUSA TV9* — **Virginia upgrading Emergency Alert System.** Virginia is developing a new satellite−based system to warn the public about severe weather and other emergencies, Gov. Mark R. Warner said last Thursday. **The first phase of the Emergency Alert System (EAS) upgrade is scheduled for completion in September. EAS is a national system that relays messages between member radio and television stations, which can then warn the public about an immediate safety threat.** The current chain of communications is time−consuming, and the system can fail if one or more key relay stations fail to monitor or receive an EAS message or decide not to rebroadcast it. **The new system will rapidly transmit EAS messages from the president or the governor to a station or group of stations. The first phase will deploy the system to 21 sites.** "We can no longer afford to rely upon an antiquated system to provide vital emergency public warnings and protective action guidance to citizens throughout the commonwealth," Warner said. "The public safety risk is too high and the threats are too numerous."
Source: http://www.wusatv9.com/weather/weather_article.aspx?storyid= 19123

23. *August 29, Federal Computer Week* — **NYC tries cell phone finder. New York City is testing a new system that will be able to triangulate the location of cell phone callers, the next phase of its wireless 911 emergency services.** The company, which helped developed the city's Enhanced 911 (E911) service in 1995, was hired by the police department to be the systems integrator and project manager for the cell phone locator test. **Currently, city dispatchers or call agents can only see a caller's phone number. Dale said when Phase II of the wireless E911 service is fully operational, which could be later this year or early next year, dispatchers will see a wireless caller's phone number, location data associated with that phone, a time stamp and the age of the last positioning report for that phone.** The city presents challenges because of its skyscrapers and underground subways, he said, but he added that advanced technologies, including cell phones equipped with global positioning satellite antennas, are improving the accuracy of a caller's position. **New York City receives about 10.3 million 911 emergency calls from landline and wireless phones each year, for an average of about 33,000 calls daily,** Dale said. On Aug. 14, the day of the power blackout

that blanketed a good deal of New York, and parts of the Midwest and Canada, New York City received 90,000 emergency calls, Dale said.
Source: http://www.fcw.com/geb/articles/2003/0825/web−nyc−08−29−03.a sp

24. *August 27, Government Technology* — **Pennsylvania DEP launches high−tech system.** On behalf of Pennsylvania Governor Edward G. Rendell, Department of Environmental Protection (DEP) Secretary Kathleen A. McGinty announced implementation of the emAlert Emergency Notification System, a 21st−century plan to enhance homeland security and protect Pennsylvania residents from environmental dangers. **"The emAlert Emergency Notification System links DEP electronically with the operators of critical infrastructure facilities throughout Pennsylvania," McGinty said. "This system ensures that people operating these vital facilities will know what they need to do to protect our citizens and our environment in the event of an emergency." The emAlert system is connected to six primary types of facilities: nuclear power plants, conventional fuel power plants, public water supplies, sewage treatment plants, high−hazard dams and large, above−ground storage tanks.** These facilities are located at more than 5,000 sites throughout Pennsylvania. An emAlert Emergency Notification System message will give these operators pertinent details on any event that triggers the system, such as an accident or natural disaster, and safety information specific to the particular event that occurs.
Source: http://www.govtech.net/news/news.php?id=2003.08.27−65785

[Return to top]

Information and Telecommunications Sector

25. *August 29, TechWeb* — **Accused MSBlaster creator placed under house detention. A teenager has admitted creating a copycat of the MSBlaster worm**, Seattle−based U.S. Attorney John McKay said Friday, August 29. Jeffrey Lee Parson, 18, of Hopkins, MN, was arrested early Friday morning on one count of intentionally causing or attempting to cause damage to a computer. Parson was placed under house detention and is being monitored electronically, said McKay. All computers in his home were seized by the FBI, and he has been denied access to the Internet. Parson is accused of modifying the original MSBlaster worm, and a variant, Blaster.B. The variant shared the same destructive characteristics as its parent, attacking PCs which had not been patched against a vulnerability in the Windows operating system. **The worm, which according to security firm Symantec infected more than 500,000 systems worldwide, caused some computers to constantly reboot, snarled enterprise network and Internet traffic**, and forced Microsoft to take the unusual step of disabling one of the addresses used to connect with its WindowsUpdate service. **Estimates by analysts as to the damage done by MSBlaster and its follow−ups range as high as $1.3 billion**.
Source: http://www.techweb.com/wire/story/TWB20030829S0007

26. *August 29, Government Technology* — **Case Western unveils free, public wireless service. Case Western Reserve University is opening more than 1,230 wireless access points September 1, providing free Internet access to faculty, students, staff and visitors**. "This is the first phase of blanketing Cleveland, OH, with free wireless Internet access −− a project we call OneCleveland," said Lev Gonick, vice president of information technology services and chief information officer at Case Western. Faculty, staff, students and visitors can take

advantage of voice and streaming video applications, access to e−curriculums and other university services from virtually anywhere on campus or in University Circle. **OneCleveland is committed to creating a seamless, digital infrastructure for the residents, businesses and institutions of Northeast Ohio**. In addition, design students at the Cleveland Institute of Art, in collaboration with students at the Case School of Engineering, are developing global positioning systems (GPS) applications incorporating text, video, audio, and even speech recognition, to allow students and visitors to take self−guided tours around University Circle using their own personal digital assistants (PDA).
Source: http://www.govtech.net/news/news.php?id=2003.08.29−66134

Internet Alert Dashboard

Current Alert Levels

AlertCon: 2 out of 4 https://gtoc.iss.net	Security Focus ThreatCon: 2 out of 4 http://analyzer.securityfocus.com/

Current Virus and Port Attacks

Virus:	#1 Virus in the United States: **WORM LOVGATE.G** Source: http://wtc.trendmicro.com/wtc/wmap.html, Trend World Micro Virus Tracking Center [Infected Computers, North America, Past 24 hours, #1 in United States]
Top 10 Target Ports	135 (epmap), 1434 (ms−sql−m), 445 (microsoft−ds), 137 (netbios−ns), 3389 (ms−term−services), 80 (www), 443 (https), 554 (rtsp), 1433 (ms−sql−s), 139 (netbios−ssn) Source: http://isc.incidents.org/top10.html; Internet Storm Center

[Return to top]

General Sector

27. *August 29, New York Times* — **Blast in Iraq kills a leading Shiite cleric. A huge car bomb killed the most prominent Shiite cleric cooperating with American forces in Iraq Friday, August 29, exploding outside the faith's holiest shrine in an attack that hospital officials said killed at least 95 people and wounded more than 140**. The death of the cleric, Ayatollah Mohammed Bakr Al−Hakim, who in exile had been a leading opponent of Saddam Hussein and was one of the four revered clerics holding sway over the Shiite Muslim faithful, sent a wave of fear coursing through Iraq's majority Shiite population. The bomb went off just as the ayatollah's motorcade was pulling away from the shrine, which includes a gold−domed inner sanctuary containing what is believed to be the tomb of the Imam Ali, the founder of Shiism. At the time of the blast, thousands of worshipers were attending Friday prayers in an outer courtyard paved in white marble. Shiites make up some 65 percent of the country's population of 25 million. **The consent of men like Ayatollah Hakim, whose brother serves on the governing council, has been a crucial factor in keeping the Shiite community behind the**

American effort.
Source: http://www.nytimes.com/2003/08/29/international/worldspecial/29CND−IRAQ.html?hp

[Return to top]

DHS/IAIP Products &Contact Information

The Department of Homeland Security's Information Analysis and Infrastructure Protection (IAIP) serves as a national critical infrastructure threat assessment, warning, vulnerability entity. The IAIP provides a range of bulletins and advisories of interest to information system security and professionals and those involved in protecting public and private infrastructures. By visiting the IAIP web−site (http://www.nipc.gov), one can quickly access any of the following DHS/IAIP products:

DHS/IAIP Warnings − DHS/IAIP Assessements, Advisories, and Alerts: DHS/IAIP produces three levels of infrastructure warnings. Collectively, these threat warning products will be based on material that is significant, credible, timely, and that address cyber and/or infrastructure dimensions with possibly significant impact.

DHS/IAIP Publications − DHS/IAIP Daily Reports, CyberNotes, Information Bulletins, and other publications

DHS/IAIP Daily Reports Archive − Access past DHS/IAIP Daily Open Source Infrastructure Reports

DHS/IAIP Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	nipcdailyadmin@mail.nipc.osis.gov or contact the DHS/IAIP Daily Report Team at 703−883−6631
Subscription and Distribution Information	Send mail to nipcdailyadmin@mail.nipc.osis.gov or contact the DHS/IAIP Daily Report Team at 703−883−6631 for more information.

Contact DHS/IAIP

To report any incidents or to request information from DHS/IAIP, contact the DHS/IAIP Watch at nipc.watch@fbi.gov or call 202−323−3204.

DHS/IAIP Disclaimer